基于中国剩余定理的区块链投票场景签名方案 *

王利朋 [1]，胡明生 [1†]，贾志娟 [1]，公　备 [2]，张家蕾 [1]

(1. 郑州师范学院 信息科学与技术学院，郑州 450044; 2. 北京工业大学 计算机学院，北京 100124)

摘　要：基于区块链的投票系统可用于信用评估、身份验证等场景。相应的电子投票协议的底层密码学技术主要基于盲签名、环签名、代理签名进行实现，然而传统的上述签名算法在应用到区块链时可能会出现依赖中心节点、效率低下等问题。基于中国孙子定理提出了一种适用于区块链投票场景的门限签名方案，通过成员之间协作，生成份额签名并合成签名。签名方法支持节点加入和退出，签名过程无须中心节点参与，提升了方案的可用性；加入了对通信数据的验证功能，同时在通信过程中不暴露密钥信息，保证了数据在区块链不安全通信信道传输时的安全性；算法优化了通信效率，不仅节省了网络带宽资源，同时提升了系统吞吐率。安全性分析表明，攻击难度等价于求解离散对数问题，能够有效抵抗冒名攻击。计算复杂度分析表明，算法计算量较低，能够有效适配到区块链应用场景。

关键词：区块链；可信计算；门限签名；中国孙子定理

中图分类号：TP393.08　　doi: 10.19734/j.issn.1001-3695.2018.08.0566

Signature scheme applying on blockchain voting scene based on Chinese remainder theorem

Wang Lipeng[1], Hu Mingsheng[1†], Jia Zhijuan[1], Gong Bei[2], Zhang Jialei[1]

(1. *School of Information Science & Technology*, *Zhengzhou Normal University*, *Zhengzhou* 450044, *China*; 2. *College of Computer Sciences*, *Beijing University of Technology*, *Beijing* 100124, *China*)

Abstract: The voting schemes based on blockchain are applicable for credit evaluation and identity verification. The underlying cryptographic schemes of the corresponding electronic voting protocols mainly include blind signature, ring signature and proxy signature. However, traditional aforementioned algorithms may arise dependence of dealers and inefficiency when applied to blockchain. Based on the Chinese Remainder Theorem, the paper proposed a threshold signature scheme for the voting scenes based on blockchain. Through cooperation, the share signatures synthesized the final signature. The proposed scheme supported the nodes join/leave behaviors. It also excluded the dealers from participation to improve the availability. The new scheme was able to verify the data, and did not expose any key information during data transmission. The proposed algorithm with high efficiency reduced the network bandwidth requirements to increase throughput. Security analysis shows that the new scheme for solving the discrete logarithm can resist impersonation attacks. Computational complexity analysis shows that the proposed algorithm with low computational cost can fit into the blockchain scenario effectively.

Key words: blockchain; confidential computation; threshold signature; Chinese remainder theorem

0　引言

区块链是一种记录交易历史的分布式数据库技术，具有去中心化、匿名化、去信任化等特征，解决了不同节点间的数据可信问题，在电子货币、金融投资、物联网、医疗、能源互联网等领域得到迅速发展。区块链主要分为三类，即公有链、联盟链和私有链，目前出现了联盟链和私有链上基于区块链的电子投票系统，用于信用评估、决策制定等场景。电子投票系统所采用的投票协议主要用于解决互联网环境下投票流程中的安全性问题，即满足投票的合法性、匿名性、计票完整性、不可伪造性、不可重复性、不可窜改性等要求。电子投票协议的底层密码学技术主要包含盲签名、环签名、代理签名这 3 种，可用于审核身份、确保投票内容可信等场景[1]。本文致力于研究一种区块链在线投票场景下的环签名方案，通过协调各投票参与方，保证投票过程的公正性和正确性，并允许新成员加入，同时允许撤销签名。相对于其他投票系统，基于区块链的投票应用存在不可窜改、不可抵赖的特性，而且其投票过程完全依据规约自动化执行，无须人工参与，其可信机制具备天然中立性和安全性，具有极高的应用前景。

当前主流的门限签名方案，按照密钥分发方式不同，主要分为有可信中心的门限签名和无可信中心的门限签名方案。有可信中心的门限签名方案存在管理节点，并承担大部分可信认证任务，然而它也是整个算法的性能瓶颈。对于无可信中心的门限签名方案，各个节点高度自治，其代价就是增加了网络的总体计算量。在区块链中基于签名算法实现投票协议时，基于可信中心的群签名方案会面临可信中心节点选择以及中心节点存储数据泄露问题；区块链作为一种去中

收稿日期：2018-08-31；**修回日期：**2018-10-10　　**基金项目：**国家自然科学基金资助项目（U1304614，U1204703）；河南省教育科学“十三五”规划一般课题资助项目（2018）-JKGHYB-0279）；郑州市创新型科技人才队伍建设工程基金资助项目（131PCXTD597）；河南省科技攻关项目（162102310238）

作者简介：王利朋（1987-），男，河南卫辉人，硕士，主要研究方向为虚拟化安全、云存储、并行计算；胡明生（1973-），男（通信作者），河南新县人，教授，博士，主要研究方向为人工智能、数据挖掘（hero_jack@163.com）；贾志娟（1973-），女，河南郑州人，教授，硕士，主要研究方向为软件工程；公备（1984-），男，山东临沂人，教授，博士，主要研究方向为信息安全、可信计算；张家蕾（1992-）女，河南洛阳人，硕士，主要研究方向为密码学、量子密码.

心化的网络结构，签名算法在适配该场景时，需要设计成一种去中心化的算法结构；此外，当区块链网络中节点不可用时，需要签名算法能够撤销用户签名。如何设计这样一种安全的、去中心化的、可撤销签名的门限签名方案是本文重点研究的问题。

由于区块链网络的异构性，为了提高服务效率，基于区块链的门限签名方案，其计算资源需求量要小，同时能够提供复杂场景下高安全性服务。在发起投票时，需要尽量减少通信次数，减少带宽需求量。当投票节点出现故障或新成员加入时，需要通过较少的计算量，高效地完成相关操作。如何设计这样一种计算资源和通信资源需求量较少的签名方案是适配到区块链应用场景的重要前提。

2004 年，Tzer-Shyong 等人将椭圆曲线加密所需较短的密钥特征与 (t,n) 门限方法集成，提出了一种新的签名方案，但没有给出身份追踪和撤销操作[2]。文献[3]对上述方案的密钥生成方式进行了改进，使得合谋攻击困难度等价于椭圆曲线离散对数困难度。文献[4]提出的门限签名方案，能够有效抵御 t 个成员合谋伪造签名的攻击。上述方法是基于 Shamir 秘密共享技术实现的门限签名方案，后面也出现了其他一些秘密共享技术。

文献[5]基于双线性映射和秘密共享思想提出了一种基于身份秘密的门限签名方案，采用基于身份的 t-out-of-n 秘密共享算法提升了算法的执行效率。文献[6]提出了一种离散对数难度的门限签名方案，能够有效抵抗针对秘密共享技术的攻击手段。文献[7]的门限群签名方案，具有较短的密钥长度、较低的计算负载和带宽需求。文献[8，9]提出了基于 ECDSA 门限签名系统，s 个参与者重构密钥，但却需要 $2s+1$ 个参与者才能签名。Goldfeder 等人[10]提出利用门限签名技术实现比特币密钥的多方控制功能，利用门限密码学技术实现密钥的可信管理。文献[11]基于可视密码学提出了一种秘密共享方案，能够有效抵御针对秘密的暴力破解。

近些年来，出现了基于中国孙子定理的秘密分享方案[12~14]，其中，Asmuth 和 Bloom 提出的 Asmuth-Bloom 门限秘密共享方案[15]，与基于 Shamir 秘密共享技术相比，计算量较小，但在不安全的通信信道中传输数据的时候，该方案不能保证数据的安全性。文献[16]提出了一种将 EIGamal 机制与 Asmuth-Bloom 门限秘密共享相结合的方案，能够防止秘密份额在传播过程中被窜改。文献[17]的方案能够有效地控制计算过程中的数据长度，具有良好的匿名性和防伪造性，然而必须依赖可信中心进行密钥分发。

针对现有研究问题，本文基于中国孙子定理提出了一种区块链上的门限签名方案，攻击难度等价于求解离散对数问题。为了更好地适配区块链网络，满足其去中心化、通信信道异构化的特征要求，本文提出的签名方法支持节点加入和退出，签名过程无须中心节点参与。此外本方案加入了对通信数据验证功能，同时在通信过程中不暴露密钥信息，能够有效抵抗冒名攻击。针对区块链应用场景，本文签名算法优化了通信次数，不仅节省了网络通信资源，同时提升了系统吞吐率。与现有门限签名算法相比，本方案在签名生成和签名验证两个方面，计算复杂度较低。

1 背景知识

1.1 数字签名

数字签名是利用密码学技术实现的用于确认数据单元来源或数据完整性的密码保护技术，主要用于非对称密钥加密与数字摘要等场景。典型的数字签名过程，首先由本人进行签名，其他人可以对其进行验证，且签名过程仅对当前验证实体有效，步骤如下所示[18]：

$G(p)\xrightarrow{\text{生成密钥}}(sk,pk)$,其中 sk 为私钥,而 pk 为公钥。

$S(sk,m)\xrightarrow{\text{生成签名}}sig$,其中 m 为明文消息, sig 为生成的签名信息。

$Verify(pk,m,sig)\xrightarrow{\text{验证签名}}\{\text{True,False}\}$,根据公钥、明文和签名信息验证数据是否完整。

目前常用的签名算法主要有椭圆曲线数字签名算法和部分盲签名算法。椭圆曲线数字签名算法主要是基于椭圆曲线离散对数难题而设计，因此其安全性主要依赖于椭圆曲线解题难度。部分盲签名算法由 Abe 等人[19]在 1996 年提出，算法的主要思想是除了事先与被签名者协商好的共识消息外，签名者无法获得所签消息的内容，从而实现保护被签名者隐私的功能。

1.2 秘密共享协议

秘密共享概念最早由 Shamir[20]和 Blackey[21]提出，该思想是将秘密以适当方法拆分为 N 份，并将每份秘密发送给不同参与者进行管理，在恢复秘密时，需要参与方个数至少要等于某一个门限值才能恢复出消息内容。经典的秘密共享算法有 Shamir 算法和基于中国孙子定理的 Asmuth-Bloom 算法。

1.2.1 Shamir 算法

Shamir (k,n) 秘密共享算法将秘密 S 分为 n 个子秘密，任意 k 个子秘密都可以恢复出 S ，而任意 $k-1$ 个子秘密无法恢复出 S 。步骤分为以下三步：

a)初始化。假设 n 个参与者 $(P_1,...P_n)$ ，门限值为 k ， p 为素数，可信中心编码范围为有限域 $\text{GF}(p)$ ，每个参与者编号为 $x_i\in\text{GF(p)}(i=1,2,...n)$ 。

b) 加密。可信中心选择 $k-1$ 次多项式 $f(x)=a_0+a_1x+a_2x^2+...+a_{k-1}x^{k-1}$ ，其中 $a_i\in\text{GF}(P)(i=1,2,...,k-1)$ ， $a_0=S$ ，将每个 $x_i\in\text{GF(p)}(i=1,2,...n)$ 带入上述等式，分别得到 $(x_1,f(x_1)),...,(x_n,f(x_n))$ ，并将这些信息对发送给各参与者。

c)解密。 n 个参与者任选 k 对消息，通过拉格朗日插值公式重构出多项式 $f(x)$ ，并求解出 $f(0)=a_0=S$ 。

1.2.2 Asmuth-Bloom 算法

a) 初始化。对于一个由 n 个成员构成的集合 $Q=\{Q_1,Q_2,...,Q_n\}$ ，门限值是 t ，秘密是 s ，选取一个大素数 p ($p>s$)，以及 n 个整数 $\{d_1,d_2,...,d_n\}$ ，且满足以下条件：

(a) $d_1,d_2,....d_n$ 严格单调递增；

(b) $\{(d_i,d_j)=1\,|\,i\neq j\}$;

(c) $\{(d_i,p)=1\,|\,i=1,2,...,n\}$;

(d) $\prod_{i=1}^{t}d_i>p\prod_{i=1}^{t-1}d_{n-i+1}$ 。

b)产生秘密份额。令 $D=\prod_{i=1}^{t}d_i$ ，可知 D/p 大于任意 $t-1$ 个 d_i 之积，随机选择一个整数 r ，其中 $r\in[0,\frac{D}{p}-1]$ ，计算 $s'=s+rp$ ，可知 $s'\in[0,D-1]$ ，对秘密进行分割，即为 $s_i\equiv s'\bmod d_i$ ，其中 $i=1,2,...,n$ 。

c)秘密恢复。任何 t 个成员可以交换各自的秘密份额来恢复出秘密 s ，这里假设参与者提交的秘密份额为 $s_1,s_2,...,s_t$ ，进而构建出同余方程组：

$$\begin{cases}s'=s_1\bmod d_1\\ s'=s_2\bmod d_2\\ \quad\cdots\\ s'=s_t\bmod d_t\end{cases}$$

根据中国孙子定理可知，该方程组在 $[0,d_1d_2...d_t]$ 中有唯一解，且其解为 $s'=\sum_{i=1}^{t}\frac{D}{d_i}\bullet b_i\bullet s_i \bmod D$，其中 b_i 满足：

$$\frac{D}{d_i}\bullet b_i\equiv 1(\bmod d_i)\text{ , } i=1,2,...t \text{ 。}$$

从上式可得到秘密 $s=s'-rp$ 。

2　本文方案

2.1　区块链门限签名系统架构

本文基于中国孙子定理提出了一种区块链上无中心的 (t,n) 门限签名方案，区块链 (t,n) 门限签名算法参与方主要包括了三个角色，分别是区块链节点(Q)、签名验证者(SV)和签名合成者 （ SC)。

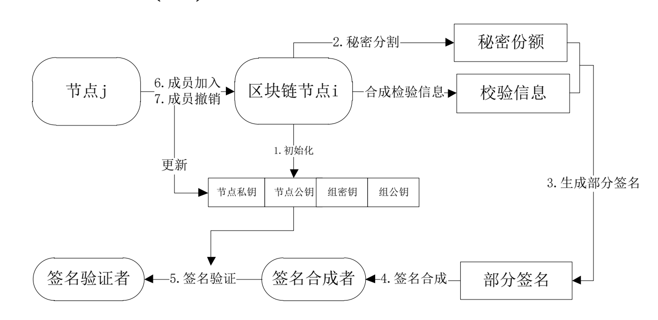


图 1　区块链门限签名方案架构图

Fig 1　Architecture of the proposed scheme

如图 1 所示，区块链 (t,n) 门限签名系统包括了初始化、秘密分割、生成部分签名、签名合成、签名验证、成员加入和成员撤销等七个步骤，具体内容如下。

a)生成签名算法所需的公共参数，同时各个节点生成自己的私钥信息和公共信息，并向网络中其他节点广播其公共信息。

b)基于中国孙子定理对节点秘密信息进行切割，分割后的秘密份额广播给其他节点，以供其他节点生成部分签名。

c)各个节点对接收到的秘密份额根据中国孙子定理求解秘密信息，结合其密钥生成部分签名，并将其广播给签名合成者。

签名合成者对接收到部分签名进行合成，这里只需要 t 份部分签名即可合成最终签名，并将最终签名发送给签名验证者进行验证。具体在区块链应用中，这里的每个节点均可以作为签名合成者，也可以作为签名验证者。

d)签名验证者对合成的签名信息进行验证，验证通过后，即可向用户反馈签名结果。

e)新成员加入时，区块链中各个节点均可以收到相关消息，进而发起成员加入流程。

f)当某一节点离开区块链网络时，区块链应用实现保证了各个节点均可以收到该节点退出信息，进而发起签名撤销流程。

需要说明的是，绝大部分区块链应用基于异构网络进行构建，而且缺少一个可信中心对资源进行优化调度，因此对签名方案的鲁棒性和安全性要求较高，需要其满足区块链的去中心化、通信信道异构化的特征要求。为了更好地适配区块链应用场景，也需要签名算法支持节点加入和退出，以提升方案的可用性。本方案的签名算法能够满足上述要求，且与基于 Shamir 秘密分享协议相比，本方案的计算效率较高。由于绝大部分区块链应用是基于不安全的通信信道，可能会出现中间人攻击，进而窜改通信数据，因此本方案加入了对通信数据的验证功能，同时在通信过程中不暴露密钥信息，进一步保证了数据的安全性。

2.2　区块链门限签名系统详细设计

下面描述了区块链 (t,n) 门限签名的详细过程，为了方便论述，定义了以下符号，如表 1 所示。

表 1　区块链门限签名符号表示

Table 1　Symbols of the proposed scheme

符号	含义	符号	含义
Q	成员集	u_s	节点私钥
s_i	成员 i 的子秘密	u_p	节点公钥
c_s	组私钥	p_a	满足 Asumth-Bloom 方案的大素数
c_p	组公钥	p_k	生成组公钥的大素数
b_{ij}	秘密份额影子	M	待签名的报文
t_i	节点 i 产生的部分签名	t	合成签名

1）初始化

设区块链中节点集为 $Q=\{Q_1,Q_2,...,Q_n\}$，一共 n 个成员，其中门限值为 t 。选择两个大素数 p_a 和 p_k，正整数序列 $d=\{d_1,d_2,...,d_n\}$ 以及有限域 Z_{p_k} 上的生成元 g，其中 p_a 和 $d=\{d_1,d_2,...,d_n\}$ 满足 Asumth-Bloom 方案的要求。需要注意的是，$\{n,t,p_a,p_k,d,g\}$ 为公知信息，各个节点均可以获知到该内容。

节点 Q_i 随机生成节点私钥 $u_s^i\in Z_{p_k}$，用于密钥分享的成员密钥 s_i 和对应的 A_i，令 $D=\prod_{i=1}^{t}d_i$，其满足：

$$0<s_i<[p_a/n]$$

$$0\le A_i\le[(D/p_a-1)/n]$$

节点 Q_i 计算得到 $c_p^i{}'=g^{s_i}$，同时得到节点公钥 $u_p^i=g^{u_s^i} \bmod p_k$，并将 $\{g^A,c_p^i{}',u_p^i\}$ 广播给其他节点，在节点获取到其他节点发送的消息后，计算得到组公钥：

$$c_p=\prod_{i=1}^{n}c_p^i{}'\equiv g^{\sum_{i=1}^{n}s_i} \bmod p_k$$

而组私钥为

$$c_s=\sum_{i=1}^{n}s_i$$

2）秘密分割

节点 Q_i 发送给节点 Q_j 的秘密份额 b_{ij} 的计算公式如下：

$$S_i'=s_i+A_ip_a$$

$$b_{ij}\equiv S_i' \bmod d_j$$

b_{ij} 将会被广播给其他节点，为了保证信息在传递过程中不被恶意窜改，需要对其进行验证。Q_i 生成的校验信息为 a_i 和 β_{ij}，其计算公式如下：

$$a_i=g^{S_i'} \bmod p_k$$

$$r_{ij}=(S_i'-b_{ij})/d_j$$

$$\beta_{ij}=g^{r_{ij}} \bmod p_k$$

节点 Q_i 将信息 $\{b_{ij},a_i,\beta_{ij}\}$ 公布给其他节点。假设此时节点 Q_j 收到上述信息，将进行校验，以确保数据的完整性，其校验公式为

$$[(g^{b_{ij}} \bmod p_k)(\beta_{ij}^{\ d_j} \bmod p_k)] \bmod p_k=a_i$$

如果验证通过，说明消息在传送信道中并没有被窜改，消息内容可信，否则区块链节点 Q_j 会要求节点 Q_i 重传消息。

3）生成部分签名

当节点 Q_j 检验成功消息后，首先计算 V_j，计算公式如下：

$$V_j \equiv \sum_{i=1}^{n} b_{ij} \bmod d_j \ ,$$

由于 $b_{ij} \equiv S_i' \bmod d_j$，故可得到：

$$V_j \equiv \sum_{i=1}^{n} S_i' \bmod d_j \ 。$$

计算出上述结果后，将相关信息发送给签名合成者，每个节点可计算得到

$$W_i = \frac{D}{d_i} \bullet b_i \bullet V_i \bmod D \ ,$$

其中 b_i 由下式计算得到

$$\frac{D}{d_i} \bullet b_i \equiv 1 \bmod d_i \ , \ i = 1,2,...,t$$

然后对于报文 M，计算其对应的部分签名 t_i：

$$\begin{aligned} u &\equiv g^{\sum_{i=1}^{t} u_s^i} \bmod p_k \\ &= \prod_{i=1}^{t} g^{u_s^i} \bmod p_k \\ &= \prod_{i=1}^{t} u_p^i \bmod p_k \end{aligned}$$

$$t_i = u_s^i M + u W_i$$

得到部分签名 t_i 后，将 $\{M,u,t_i\}$ 发送给签名合成者进行签名合成。

4）签名合成

签名合成者接收到份额签名 $\{M,u,t_i\}$ 后，进行签名合成操作。需要注意的是，在区块链场景中，每个节点均可以承担签名合成者角色。

合成签名 t 的计算公式如下所示：

$$t = \left(\sum_{i=1}^{t} t_i \bmod D \right) \bmod p_a$$

签名合成者将 $\{M,u,t\}$ 发送给签名验证者进行校验，进行签名验证。

5）签名验证

签名验证者得到签名信息 $\{M,u,t\}$ 后，需要对其进行验证，如果验证不通过，则意味着签名信息与明文信息不对应，说明消息已经被窜改。需要说明的是，签名验证者可以是区块链网络中任一个节点。验证公式如下：

$$g^t = u^M c_p{}^u \bmod p_k$$

6）成员加入

当某一节点 Q_{n+1} 要加入到区块链网络时，此时随机生成节点私钥 $u_s^{n+1} \in Z_{p_k}$，用于密钥分享的成员密钥 s_{n+1} 和对应的 A_{n+1}，并计算出对应的 $c_p^{n+1}{}' = g^{s_{n+1}}$ 和 $u_p^{n+1} = g^{u_s^{n+1}} \bmod p_k$，将 $\{c_p^{n+1}{}', u_p^{n+1}\}$ 公布给其他节点，并更新组公钥 $c_p{}'$，其更新公式如下所示：

$$c_p{}' = \prod_{i=1}^{n+1} c_p^i{}' = c_p^{n+1}{}' \prod_{i=1}^{n} c_p^i{}' = c_p^{n+1}{}' c_p$$

从上可知，更新组公钥只需要执行一次乘法运算即可，更新效率较高。

在进行签名时，从步骤 2 秘密分割开始执行。

7）成员撤销

某一节点 Q_j 离开网络时，区块链中其他节点均会收到该节点退出的消息，此时其他节点 Q_i 由于已经存储了节点 j 的公钥等其他信息，更新组公钥 $c_p{}'$ 的等式如下：

$$c_p{}' = c_p / c_p^j{}'$$

从上可知，在更新组公钥时，只需在本节点执行一次除法操作即可，无须再与其他节点进行交互，节省了网络带宽资源，同时提升了更新效率。

由于 $d = \{d_1, d_2, ..., d_n\}$ 为公知消息，节点 Q_i 删除 d_j 和 b_{ij} 的内容，在发起签名的时候，只需要从第三步生成部分签名开始执行。

3　安全性分析

3.1　正确性证明

定理 1　节点 i 收到秘密分割消息后，消息验证等式 $[(g^{b_{ij}} \bmod p_k)(\beta_{ij}{}^{d_j} \bmod p_k)] \bmod p_k = a_i$ 成立。

证明　由于 $\beta_{ij} = g^{r_{ij}} \bmod p_k$，故：

$$\begin{aligned} & [(g^{b_{ij}} \bmod p_k)(\beta_{ij}{}^{d_j} \bmod p_k)] \bmod p_k \\ = & [(g^{b_{ij}} \bmod p_k)((g^{r_{ij}} \bmod p_k)^{d_j} \bmod p_k)] \bmod p_k \end{aligned}$$

由于 p_k 为一个大素数，所以可知

$$\begin{aligned} & [(g^{b_{ij}} \bmod p_k)((g^{r_{ij}} \bmod p_k)^{d_j} \bmod p_k)] \bmod p_k \\ = & [(g^{b_{ij}} \bmod p_k)(g^{r_{ij} d_j} \bmod p_k)] \bmod p_k \\ = & (g^{b_{ij}} g^{r_{ij} d_j}) \bmod p_k \\ = & (g^{b_{ij} + r_{ij} d_j}) \bmod p_k \end{aligned}$$

由于 $r_{ij} = (S_i' - b_{ij}) / d_j$，所以可知

$$\begin{aligned} & [(g^{b_{ij}} \bmod p_k)(\beta_{ij}{}^{d_j} \bmod p_k)] \bmod p_k \\ = & (g^{b_{ij} + r_{ij} d_j}) \bmod p_k \\ = & (g^{b_{ij} + S_i' - b_{ij}}) \bmod p_k \\ = & g^{S_i'} \bmod p_k \\ = & a_i \end{aligned} \ 。$$

故原式得证。

定理 2　节点收到其他 t 个节点发送的影子份额时，能够恢复出最终秘密且其值唯一。

证明　由于 $S_i' = s_i + A_i p_a$，s_i 为各个节点生成的子秘密，$\sum_{i=1}^{n} S_i'$ 可视为合成后的秘密。由于 $V_j \equiv \sum_{i=1}^{n} S_i' \bmod d_j, j = 1,2,..n$，不妨做如下变换：

$$X = \sum_{i=1}^{n} S_i' \equiv V_i \bmod d_i , i = 1,2,...,t \ ,$$

求解本方案的合成秘密即等价于求解上述同余式组。

由于 $0 < s_i < [p_a / n]$，$0 \le A_i \le [(D / p_a - 1) / n]$，因此可以得到：

$$\begin{aligned} X &= \sum_{i=1}^{n} S_i' = \sum_{i=1}^{n} (s_i + A_i p_a) = \sum_{i=1}^{n} s_i + \sum_{i=1}^{n} (A_i p_a) \\ &< (p_a / n) \times n + ((D / p_a - 1) / n) \times n p_a \\ &= p_a + D - p_a \\ &= D \end{aligned}$$

求解上述同余式组的解为

$$\begin{aligned} X &= \sum_{i=1}^{t} \frac{D}{d_i} \bullet b_i \bullet V_i \bmod D \\ &= \sum_{i=1}^{t} \left(\frac{D}{d_i} \bullet b_i \bullet V_i \bmod D \right) \bmod D \ , \\ &= \sum_{i=1}^{t} W_i \bmod D \end{aligned}$$

其中：$\frac{D}{d_i}\bullet b_i \equiv 1 \bmod d_i$，$i=1,2,\dots,t$。

由于 $X<D$，故上述同余方程组有解，且其值唯一。

定理 3　合成签名时，签名验证公式 $g^t = u^M c_p{}^u \bmod p_k$ 成立

证明　由于

$$t=\left(\sum_{i=1}^{t} t_i \bmod D\right) \bmod p_a,$$

$$u \equiv \prod_{i=1}^{t} u_p^i \bmod p_k,$$

$$t_i = u_s^i M + uW_i,$$

可得

$$\begin{aligned} t &= \left(\sum_{i=1}^{t} t_i \bmod D\right) \bmod p_a \\ &= \left(\sum_{i=1}^{t}\left(u_s^i M + uW_i\right) \bmod D\right) \bmod p_a \\ &= \left(M\sum_{i=1}^{t} u_s^i + u\sum_{i=1}^{t} W_i \bmod D\right) \bmod p_a \\ &= \left(M\sum_{i=1}^{t} u_s^i + uX\right) \bmod p_a \end{aligned}$$

又因为

$$\begin{aligned} c_s &= \sum_{i=1}^{n} s_i = \sum_{i=1}^{n}(S_i{}' - A_i p_a) \\ &= \sum_{i=1}^{n}(S_i{}') - \sum_{i=1}^{n}(A_i p_a) \\ &= X - \sum_{i=1}^{n}(A_i p_a) \end{aligned}$$

所以可知 $X=\sum_{i=1}^{n}(A_i p_a)+c_s$。

又因为

$$t \equiv \left(M\sum_{i=1}^{t} u_s^i + uX\right) \bmod p_a$$

所以可得

$$\begin{aligned} t &\equiv \left(M\sum_{i=1}^{t} u_s^i + uX\right) \bmod p_a \\ &= \left(M\sum_{i=1}^{t} u_s^i + up_a\sum_{i=1}^{n}(A_i) + uc_s\right) \bmod p_a \\ &= \left(M\sum_{i=1}^{t} u_s^i + uc_s\right) \bmod p_a \end{aligned}$$

由于 $u \equiv \prod_{i=1}^{t} u_p^i \bmod p_k = g^{\sum_{i=1}^{t} u_s^i} \bmod p_k$，

且 $c_p = \prod_{i=1}^{n} c_p^i{}' \equiv g^{\sum_{i=1}^{n} s_i} \bmod p_k$，可得到：

$$\begin{aligned} & u^M c_p{}^u \bmod p_k \\ &= g^{M\sum_{i=1}^{t} u_s^i} g^{u\sum_{i=1}^{n} s_i} \bmod p_k \\ &= g^{M\sum_{i=1}^{t} u_s^i + u\sum_{i=1}^{n} s_i} \bmod p_k \\ &= g^{M\sum_{i=1}^{t} u_s^i + uc_s} \bmod p_k \end{aligned}$$

p_a 与 p_k 是两个大素数,可认为 $M\sum_{i=1}^{t} u_s^i + uc_s$ 小于 p_a，在 $t\in(0,p_a)$ 时,可以得到 $t=M\sum_{i=1}^{t} u_s^i + uc_s$,故:

$$\begin{aligned} & u^M c_p{}^u \bmod p_k \\ &= g^{M\sum_{i=1}^{t} u_s^i + uc_s} \bmod p_k \\ &= g^t \bmod p_k \end{aligned}$$

原式得证。

3.2　安全性证明

3.2.1 门限安全性分析

在区块链上实现 (t,n) 门限签名方案，对于 n 个节点的网络，至少需要 t 个节点协作才能生成最终签名。对于一个设计良好的门限签名算法，如果攻击者攻破了其中一定数量的节点，此时只要发起签名的合法节点数量大于等于 t，就不会影响最终投票结果。

对于 n 个参与者，在进行秘密分割时，区块链网络中各个节点对子秘密 s_i 进行分割，组公钥 $c_p = g^{\sum_{i=1}^{n} s_i} \bmod p_k$，而组私钥为 $c_s=\sum_{i=1}^{n} s_i$。c_p 被公开，即使第三方窃取到该消息，求解组私钥问题属于求解离散对数问题,而求解该问题是困难的。另外由于各个节点各自保存了自己的子秘密信息，在通信过程中并没有直接发送子秘密内容，除非全体成员协同作假，否则无法直接得到组私钥信息。

在生成部分签名时，此时节点会接收到消息 $\{g^{A_i}, b_{ij}, a_i, \beta_{ij}\}$，并进行校验，以确定消息内容在传输过程中没有被窜改。如果第三方窃取到该消息内容，而在知道 g^{A_i}，a_i 和 β_{ij} 内容的前提下求解 A_i，$S_i^{'}$ 和 r_{ij} 属于离散对数问题，而求解该问题是困难的。由于 $s_i = S_i{}' - A_i p_a$，故也不能根据该验证消息求解出 s_i。

校验通过后，需要至少 t 个节点发过来 b_{ij}，然后进行秘密合成。如果消息数量多于 t，此时只需从中选择出 t 组进行合成，反之，如果少于 t 组签名，根据中国孙子定理求解该同余方程组无法得到其解。

对消息进行签名，生成对应的部分签名信息 $\{M,u,t_i\}$，并发送给签名合成者，其中部分签名的生成公式为

$$\begin{aligned} t_i &= u_s^i M + uW_i \\ &= u_s^i M + W_i g^{\sum_{i=1}^{t} u_s^i} \bmod p_k \end{aligned}$$

由于 $u \equiv g^{\sum_{i=1}^{t} u_s^i} \bmod p_k$，根据 u 求解节点私钥 u_s^i 属于离散对数问题，同时也无法根据 t_i 的数值来获取到 u_s^i 的数值。

在对部分签名进行合成时，其合成公式为 $t=\left(\sum_{i=1}^{t} t_i \bmod D\right) \bmod p_a$，并将 $\{M,u,t\}$ 发送给签名验证者进行验证，验证公式为 $g^t = u^M c_p{}^u \bmod p_k$。由于在实际传输过程中，$\{M,u,t\}$ 没有包含私钥内容，即使第三方窃取该内容，也无法获取任何有意义的信息。

3.2.2 不可冒充性分析

不可冒充性是指区块链中的节点都不能冒充其他成员来生成签名信息，更高级的不可冒充性还包括了签名信息可追溯性。本方案在应用到区块链应用场景中时，由于剔除了可信中心，各节点地位相同，通过协作生成最终签名，因此可以避免传统的基于可信中心签名方案出现的可信中心冒充欺骗的问题。后文在分析不可冒充性的时候，设定任一区块链节点均可以冒充其他节点身份对发送的消息 M 进行签名。为了方便论述，这里将恶意节点定义为节点 j，被冒充的当前

节点定义为 i 。

如果成员 j 冒充成员 i，并生成自己的密钥 $s_i^{'}$，根据前面所述，根据公开的信息是无法计算出成员 i 的私钥信息。当随机生成 $s_i^{'}$，且 $s_i^{'} \neq s_i$ 时，由于组私钥为 $c_s^{'} = \sum_{i=1}^{n} s_i^{'}$，区块链各个节点均会在本地保存一份组私钥信息，如果 $s_i^{'} \neq s_i$，则必然会导致组私钥信息计算错误，导致节点 j 无法加入到签名生成流程，因此成员 j 不能通过生成其对应的密钥信息 s_j 冒充成员 i 。

如果成员 j 冒充成员 i 时，生成节点私钥 $u_s^{i}{'} \neq u_s^{i}$。由于节点公钥 $u_p^{i}{'} = g^{u_s^{i}{'}} \bmod p_k$，为了正常生成签名，必须保证 $u_p^{i}{'} = u_p^{i}$，而根据 $u_p^{i}{'}$ 计算出 $u_s^{i}{'}$ 属于求解离散对数问题，这是困难的，因此成员 j 不能通过生成其对应的节点私钥 $u_s^{i}{'}$ 冒充成员 i 。

如果成员 j 冒充成员 i 并生成 $A_i^{'} \neq A_i$ 时，由于

$$
\begin{aligned}
&\left((g^{b_{ij}^{'}} \bmod p_k)(\beta_{ij}^{'\,d_j} \bmod p_k)\right) \bmod p_k \\
&\equiv a_i{'} \\
&= g^{S_i^{''}} \bmod p_k \\
&= (g^{s_i^{'}+A_i^{'}p_a}) \bmod p_k \\
&= g^{s_i^{'}} g^{A_i^{'}p_a} \bmod p_k \\
&= g^{s_i^{'}} (g^{A_i^{'}})^{p_a} \bmod p_k
\end{aligned}
$$

可以得到

$$\beta_{ij}^{'} = g^{\frac{s_i^{'}-b_{ij}^{'}}{d_j}} (g^{A_i^{'}})^{\frac{p_a}{d_j}} \bmod p_k = g^{\frac{s_i^{'}-b_{ij}^{'}+A_i^{'}p_a}{d_j}} \bmod p_k$$

另外由于 $\beta_{ij}^{'}$ 为整数，g 为素数，可以得到

$$d_j \mid s_i^{'} - b_{ij}^{'} + A_i^{'} p_a$$

对于 $\beta_{ij} \equiv g^{\frac{s_i - b_{ij} + A_i p_a}{d_j}} \bmod p_k$，同理可得

$$d_j \mid s_i - b_{ij} + A_i p_a$$

由于 $s_i^{'}$ 不可伪造，$s_i^{'} = s_i$，所以可以得到

$$
\begin{aligned}
&d_j \mid s_i^{'} - b_{ij}^{'} + A_i^{'} p_a - 1*(s_i - b_{ij} + A_i p_a) \\
&= d_j \mid b_{ij} - b_{ij}^{'} + (A_i^{'} - A_i) p_a
\end{aligned}
$$

进而得到

$$(A_i - A_i^{'}) p_a \equiv (b_{ij} - b_{ij}^{'}) \bmod d_j$$

为了求解 $A_i^{'}$ 的数值，则需要求解 $(A_i - A_i^{'})$，又因为 p_a, d_j 互素，所以可以得到

$$
\begin{aligned}
&(p_a, d_j) \mid (b_{ij} - b_{ij}^{'}) \\
&= 1 \mid (b_{ij} - b_{ij}^{'})
\end{aligned},
$$

则 $(A_i - A_i^{'}) p_a \equiv (b_{ij} - b_{ij}^{'}) \bmod d_j$ 有解。为了保证节点 j 在生成部分签名后能够正常合成最终签名，必须使 $b_{ij} = b_{ij}^{'}$，故此时为了保证方程组有解，只能 $A_i = A_i^{'}$，与题设矛盾，故成员 j 无法生成 $A_i^{'}$ 来冒充成员 i 。

如果成员 j 冒充成员 i 并生成 $a_i^{'} \neq a_i$ 时，由于 $a_i^{'} = g^{s_i^{'}+A_i^{'}p_a} \bmod p_k$，而且 $s_i^{'}$ 与 $A_i^{'}$ 无法冒充，所以 $s_i^{'} = s_i$，$A_i^{'} = A_i$，因此 $a_i^{'} = a_i$，成员 j 无法生成 $a_i^{'}$ 来冒充成员 i 。

如果成员 j 冒充成员 i 并生成 $\beta_{ij}^{'} \neq \beta_{ij}$ 时，由于成员 j 无法冒充成员 i 并生成其对应的 $a_i^{'}$，s_i，$u_s^{i}{'}$ 以及 $A_i^{'}$，意味着此时 $a_i^{'} = a_i$，$s_i^{'} = s_i$，$u_s^{i}{'} = u_s^{i}$ 以及 $A_i^{'} = A_i$，此时可知

$$S_i^{'}{'} = s_i^{'} + A_i^{'} p_a = s_i + A_i p_a = S_i{'}$$

$$b_{ij}^{'} \equiv S_i^{'}{'} \bmod d_j = S_i{'} \bmod d_j = b_{ij}$$

$$
\begin{aligned}
&\beta_{ij}^{'} = g^{r_{ij}{'}} \bmod p_k = g^{(S_i^{'}{'}-b_{ij}^{'})/d_j} \bmod p_k \\
&= g^{(S_i^{'}-b_{ij})/d_j} \bmod p_k \\
&= \beta_{ij}
\end{aligned}
$$

所以成员 j 无法生成 $\beta_{ij}^{'}$ 来冒充成员 i 。

综上所述，本文提出的区块链 (t,n) 门限签名方案，区块链中节点均不能冒充其他成员来生成签名信息，保障了方案的安全性。

4 性能分析

4.1 效率分析

本文提出的区块链 (t,n) 门限签名算法难度等价于求解离散对数问题，为了与当前已有的签名算法进行性能对比，本文定义了以下的符号，如表 2 所示。

表 2 新方案复杂度符号表示

Table 2 Symbols of computational complexity for the proposed scheme

符号	说明
C_m	模乘计算复杂度
C_p	模幂计算复杂度
C_i	模求逆计算复杂度
C_h	哈希计算复杂度

需要说明的是由于模加法和模减法计算开销较低，这里不对其进行考察。模幂运算本质上是一种模乘运算，模幂运算可以通过蒙哥马利幂模运算进行简化，后面在对本方案进行性能评估时，模幂运算单独论述。

本部分将会分别从秘密分割、签名生成和签名验证三个方面进行效率分析，其中签名生成包括了前文论述的生成部分签名和签名合成两个步骤。另外在计算复杂度时，对同一计算任务，只统计一次。区块链 (t,n) 门限签名算法的计算复杂度如表 3 所示。

表 3 新方案的计算复杂度

Table 3 Computational complexity of the proposed scheme

步骤	计算复杂度
秘密分割	$(4n)C_p + tC_m$
签名生成	$(2t)C_p + tC_i$
签名验证	$2C_p + C_m$

为了与现有的门限签名方法进行对比，后面将从签名生成和签名验证两个角度对算法进行考察。由于现有的方法种类复杂，主要包括了基于拉格朗日插值法和基于中国孙子定理的方法，所以本文重点对基于上述两种秘密共享的门限签名算法进行性能比较。表 4 是本文区块链 (t,n) 门限签名算法

与现有算法的计算复杂度对比结果。其中本文与文献[22]是基于中国孙子定理，而文献[23，24]则是基于拉格朗日插值算法，文献[25]是基于零知识证明。

表 4 算法计算复杂度对比

Table 4　Comparison of computational complexity

方案名称	签名生成效率	签名验证效率
本文算法	$(2t)C_p + tC_i$	$2C_p + C_m$
文献[22]	$(3t)C_m + tC_p + tC_i$	$C_p + C_m$
文献[23]	$(8t+1)C_p + (2t+2)C_m$	$2C_p$
文献[24]	$(2t)C_p + (t+1)C_m + tC_h + C_i$	C_h
文献[25]	$(5t)C_p + (4t+1)C_m + tC_h$	$3C_p + 2C_m + C_i$

从表 4 可知，对于签名生成和签名验证，本文算法均要优于文献[25]，后者秘密份额包括了用户身份信息，用于授权管理和检测参与者是否存在欺骗行为，而为了保护用户身份信息，额外引入了哈希函数来盲化身份信息。同时授权子集为了进行权限管理，也引入了额外的操作，故导致其计算复杂度较高。

一般来讲，哈希函数计算复杂度一般要高于取模运算，因此在签名生成部分，文献[24]比本文算法效率低。区块链作为一种异构网络，计算资源有限，对算法执行效率要求较高。由于门限签名算法计算量主要集中在签名生成部分，而不是签名验证部分，因此提升签名生成部分效率对提升算法在区块链执行效率价值更大。因此，尽管本文算法在签名验证部分要逊于文献[23]，但由于签名生成效率较高，在适配到区块链应用场景中时，系统吞吐率仍要优于后者。

区块链作为一种去中心化的分布式网络，签名算法计算任务均匀分布到各个节点中。由于区块链各个节点的计算能力参差不齐，单独增加区块链网络某些节点的计算资源，并不能有效地提升签名算法执行效率。其中影响签名算法执行效率的关键要素是通信资源消耗量，减少通信次数可以缩短签名算法的执行时间。尽管文献[22]在签名生成和签名验证两个方面均要优于本文算法，但是文献[22]在产生签名时，生成部分签名需要生成自己的临时公钥信息，并进行广播，其他节点收到 t 个节点相关消息后才能合成最终签名，而本文算法没有相关步骤，减少了一次通信过程，不仅节省了计算资源，同时提升了合成签名的效率，有效地增加任务吞吐率。

文献[23~25]均未提供成员加入和撤销签名功能，而文献[22]没有提供撤销签名功能。由于区块链作为一种复杂网络，节点状态随机性较大，断电和故障均会导致节点不可用，因此要求签名算法均要支持签名撤销和成员加入功能，且其效率要高。本文签名算法针对区块链应用场景进行了功能和性能上优化，相比其他算法，能够更为有效地适配到区块链应用场景中。

4.2　仿真实验

仿真实验采用的操作系统为 Windows 7, Intel CPU i7-6700, Microsoft VC++ 6.0。将本文方案与文献[23]方案的执行效率进行对比，统计签名生成和签名验证两个步骤的耗时总和，时间单位为 ms。 p_a 和 p_k 均为 150 位整数，仿真实验将分别考察耗时与门限值 t 和成员数 n 之间的关系，详细的实验配置参数如下：

实验 1　成员数 $n=50$，门限值 t 分别取值为 10、15、20、25、30、35、40，考察耗时与门限值 t 之间的关系。

实验 2　门限值 $t=30$，成员数 n 分别取值为 40、45、50、55、60、65、70、75、80，考察耗时与成员数 n 之间的关系。

仿真实验结果如图 2 和 3 所示。

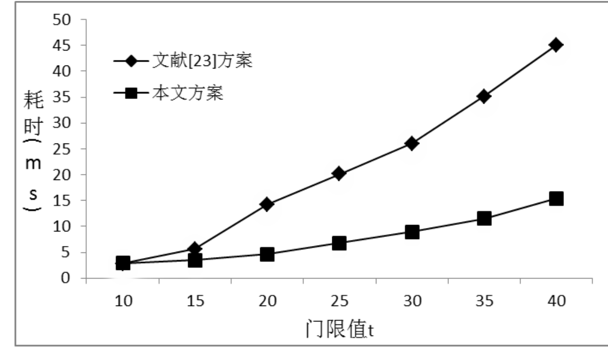


图 2　耗时与门限值 t 关系图

Fig. 2　Relationship of time consuming over the threshold t

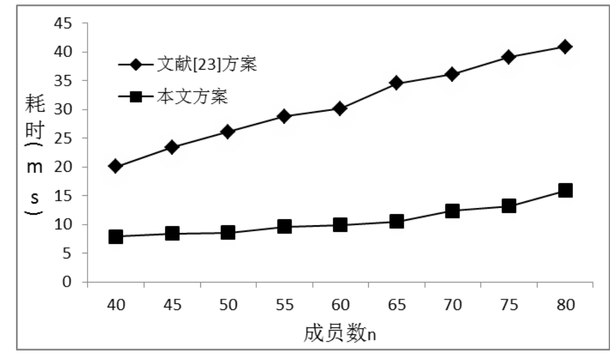


图 3　耗时与成员数 n 关系图

Fig. 3　Relationship of time consuming over the member number n

从图 2 可知，随门限值 t 的增加，本方案与文献[23]的耗时均会增加，这是由于签名生成时的计算复杂度与门限值 t 正相关。从实验数据可知，文献[23]相对于本方案，耗时较多，且随门限值 t 的增加，耗时增加速度变快。门限值 t 较小时，两种方案的耗时相近，这是由于签名生成时两者的计算复杂度，在门限值较小时其数值接近。

从图 3 可知，随成员数 n 的增加，本方案的耗时基本上保持平稳，且均小于文献[23]。综合图 2 和 3 可以进一步发现，本文算法在门限值 t 和成员数 n 发生变化时，耗时波动相比较小，性能基本保持平稳。对于区块链这种异构网络，节点数量变化频繁，而本文算法的性能并不会随之发生较大波动，具有更好的鲁棒性，能够更好地适配到区块链投票协议中。

5　结束语

区块链中应用环签名算法实现投票功能时，会面临节点不可信以及效率低下的问题，本文基于中国孙子定理提出了一种区块链上的门限签名方案，攻击难度等价于求解离散对数问题。

区块链具有去中心化、通信信道异构化的特征，在适配到区块链网络时，本方案的签名方法支持节点加入和退出，签名过程无须中心节点参与，提升了方案的可用性。由于区块链是基于不安全的通信信道进行构建，为了抵御可能出现的中间人攻击，本方案加入了对通信数据的验证功能；同时本方案在通信过程中不暴露密钥信息，保证了数据安全性。安全性分析表明，本文所提出的门限签名方案能够有效抵抗冒名攻击，克服了原生区块链系统的安全缺陷。针对区块链应用场景，本文算法优化了通信效率，节省了计算资源，提升了系统吞吐率。性能分析表明，与现有门限签名算法相比，本方案在签名生成和签名验证两个方面，计算复杂度较低，且具有较好的鲁棒性。

参考文献：

[1] 董友康，张大伟，韩臻，等．基于联盟区块链的董事会电子投票系统 [J]．网络与信息安全学报，2017, 3(12): 17-23. (Dong Youkang, Zhang Dawei, Han Zhen, *et al.* Board voting system based on the consortium blockchains [J]. Chinese Journal of Network and Information Security, 2017, 3(12): 17-23.)

[2] Chen Tzershyong, Hsiao Tsungchih, Chen Tzerlong. An efficient threshold group signature scheme [C]//Proc of IEEE Region 10 Conference Tencon.Piscataway,NJ: IEEE Press, 2004: 13-16.

[3] 彭娅．门限数字签名理论及应用研究 [D]．广州：中山大学，2010. (Peng Ya. Research on threshold digital signature theory and application [D]. Guangzhou: Sun Yat-sen University, 2010.)

[4] 谢冬，李佳佳，沈忠华．一种新的基于椭圆曲线的门限群签名方案 [J]．杭州师范大学学报:自然科学版,2013, 12(1): 57-60. (Xie Dong, Li Jiajia, Shen Zhonghua. A new threshold signature scheme based on elliptic curve crypto system [J]. Journal of Hangzhou Normal University:Nature Science Edition, 2013,12(1): 57-60.)

[5] Liu Hongwei, Xie Weixin, Yu Jianping, *et al.* Efficiency identity-based threshold group signature scheme [J]. Journal on Communications, 2009, 30 (5): 122-127.

[6] 闫杰，尹旭日，张武军．基于椭圆曲线的带门限值的群签名研究 [J]．东南大学学报:自然科学版 ，2008, 38(1): 43-46. (Yan Jie, Yin Xuri, Zhang Wujun. Research on group signature with threshold value based on elliptic curve [J]. Journal of Southeast University:Nature Science Edition , 2008, 38 (1): 43-46.)

[7] Chung Yufang, Chen Tzerlong, Chen Tzershyong, *et al.* A study on efficient group-oriented signature schemes for realistic application environment [J]. International Journal of Innovative Computing Information & Control, 2012, 8(4): 2713-2727.

[8] Gennaro R, Jarecki S, Krawczyk H, *et al.* Robust threshold DSS signatures [J]. Information and Computation, 2001, 164(1): 354-371.

[9] Gennaro R, Jarecki S, Krawczyk H, *et al.* Secure distributed key generation for discrete-log based cryptosystems [C]//Proc of International Conference on Theory and Application of Cryptographic Techniques. Berlin: Springer Press, 1999: 295-310.

[10] Goldfeder S, Gennaro R, Kalodner H. Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme [EB/OL]. (2015) [2018-07-23]. https://www. cs. princeton. edu/~stevenag/threshold_sigs. pdf.

[11] Jia Xingxing, Wang Daoshun, Nie Daxin, *et al.* Collaborative visual cryptographic schemes [J]. IEEE Trans on Circuits & Systems for Video Technology, 2018, 8(5): 1056-1070.

[12] Hou Zhengfeng, Tan Mengna. A CRT-based (t,n) threshold signature scheme without a dealer [J]. Journal of Computational Information Systems, 2015, 11 (3): 975-986.

[13] Shi Nan, Hou Zhengfeng, Tan Mengna, *et al.* A threshold encryption scheme without a dealer based on Chinese remainder theorem [C]// Proc of IEEE International Conference on Communication Software and Networks.Piscataway,NJ: IEEE Press, 2017: 90-96.

[14] 徐甫，马静谨．基于中国剩余定理的门限 RSA 签名方案的改进 [J]．电子与信息学报，2015, 37(10): 2495-2500. (Xu Pu, Ma Jingjin. Improvement of threshold RSA signature scheme based on Chinese remainder theorem [J]. Journal of Electronics & Information Technology, 2015, 37(10): 2495-2500.)

[15] Asmuth C, Bloom J. A modular approach to key safeguarding [J]. IEEE Transactions on Information Theory, 1983, 29(2): 208-210.

[16] 程宇，刘焕平．可验证的 Asmuth-Bloom 门限秘密共享方案 [J]．哈尔滨师范大学自然科学学报，2011, 27(3): 35-38. (Cheng Yu, Liu Huanping. The Asmuth-Bloom verifiable threshold sharing scheme [J]. Natural Sciences Journal of Harbin Normal University, 2011, 27(3): 35-38.)

[17] 党佳莉，俞惠芳．使用中国剩余定理的群签名方案 [J]．计算机工程, 2015, 41(2): 113-116. (Dang Jiali, Yu Huifang. Group signature scheme using Chinese remainder theorem [J]. Computer Engineering, 2015, 41(2): 113-116.)

[18] 陈思．比特币的匿名性和密钥管理研究[D]．西安:西安电子科技大学，2017. (Chen Si. Research on anonymity and key management of Bitcoin [D]. Xian: XiDian University, 2017.)

[19] Abe M, Fujisaki E. How to date blind signatures [C]//Advances in Cryptology-ASIACRYPTO. Beijing: Springer Press, 1996: 244-251.

[20] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[21] Blakley G R. Safeguarding cryptographic keys [C]//Proc of International Workshop on Managing Requirements Knowledge. New York: AFIPS Press, 1979: 313-317.

[22] 王岩，侯整风，章雪琦，等．基于中国剩余定理的动态门限签名方案 [J]．计算机应用，2018, 38(4): 1041-1045. (Wang Yan, Hou Zhengfeng, Zhang Xueqi, *et al.* Dynamic threshold signature scheme based on Chinese remainder theorem [J]. Journal of Computer Applications, 2018, 38 (4): 1041-1045.)

[23] 徐甫．基于多项式秘密共享的前摄性门限 RSA 签名方案 [J]．电子与信息学报，2016, 38(9): 2280-2286. (Xu Fu. Proactive threshold RSA signature scheme based on polynomial secret sharing [J]. Journal of Electronics & Information Technology, 2016, 38 (9): 2280-2286.)

[24] 尚光龙，曾雪松．一个无可信中心的门限群签名方案 [J]．河北北方学院学报:自然科学版，2017, 33(5): 4-8. (Shang Guanglong, Zeng Xuesong. Threshold group signature scheme without TA [J]. Journal of Hebei North University:Natural Science Edition , 2017, 33(5): 4-8.)

[25] 曹阳．基于秘密共享的数字签名方案 [J]．重庆邮电大学学报:自然科学版，2015, 27(3): 418-421. (Cao Yang. Digital signature scheme based on secret sharing [J]. Journal of Chongqing University of Posts and Telecommunications:Natural Science Edition, 2015,27(3): 418-421.)